



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,857	07/31/2003	Carey Nachenberg	20423-07776	4612

34415 7590 09/25/2007
SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER

POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
----------	--------------

2134

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

09/25/2007

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary

Application No.

10/632,857

Applicant(s)

NACHENBERG, CAREY

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 27 July 2007.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 have been examined.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

2. The applicant's amendment to the specification is accepted.
3. In light of applicant's arguments and amendments the objections 35 USC § 101 and 112 rejections cited in the previous Office Action are withdrawn.
4. Applicant's argument are directed towards the newly introduced limitations. These new limitations are addressed in the current Office Action, below.

Claim Rejections - 35 USC § 103

5. Claims 1-32 are rejected under 35 U.S.C. 103(a) as obvious over Mattsson (USPN 7120933).

Mattsson's invention discloses a method of detecting intrusion in a database.

As per claims 1, 13, 15 and 31-32, Mattsson teaches as follow:

"generating retrieval information characteristic of data sent to a retriever by the computer code in response to a retrieval command issued by the retriever, the retrieval information comprising an input vector characterizing the retrieval command" (Mattsson, col. 4 lines 36-47) and "determining whether the retrieval command is acceptable using at least some of retrieval information as an input to at least one rule and responsive to the retrieval command being not acceptable

performing at least one of the following: sending a message to a user or a computer" (Mattsson, col. 4 lines 47-59).

6. Mattsson does not explicitly recite the newly introduced limitations:

"observing a plurality of retrieval commands that access the computer code, observing a plurality of retrieval commands generated by the computer code, deriving responses to the plurality of retrieval commands generated by the computer code, deriving from the plurality of retrieval commands and the responses a set of retrieval information, the set of retrieval information comprising input vectors, characterizing the plurality of retrieval commands and converting the set of retrieval information into at least one rule for determining whether retrieval commands are acceptable".

However, as discussed below, these limitations, if not inherent, would have been at least obvious to one of the ordinary skills in the art at the time of applicant's invention.

7. It is clear that Mattsson's invention is implemented using a computer code and computer code operate based on various trigger mechanisms, e.g. procedures calls, interrupts etc. Thus, in order to generate retrieval information characteristic of data sent to a retriever by the computer code in response to a retrieval command issued by the retriever, a computer program must observe a plurality of retrieval commands that access the computer code, and responses to the plurality of retrieval commands generated by the computer code must be derived. Determining whether the retrieval command is acceptable using at least some of retrieval information as an input to at

least one rule based on the retrieval information comprising an input vector characterizing the retrieval command clearly requires observing a plurality of retrieval commands generated by the computer code, deriving from the plurality of retrieval commands and the responses a set of retrieval information, the set of retrieval information comprising input vectors and characterizing the plurality of retrieval commands. Finally, responsive to the retrieval command being not acceptable performing at least sending a message to a user or a computer is a clear indication that the set of retrieval information had to be converted into at least one rule for determining whether retrieval commands are acceptable.

8. Additionally, the examiner points out that these steps also read on a test stage of configuring a system to act in a particular way. An ordinary artisan in the art of a computer science would readily recognize that each system has different specifications and requirements. Tests are frequently conducted in the field of computer science, especially in environment that must meet high security and production requirements, in order to analyze, test and validate the behavior of the particular system according to data input/output.

Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a test stage (thus, observing a plurality of retrieval commands that access the computer code, observing a plurality of retrieval commands generated by the computer code, deriving responses to the plurality of retrieval commands generated by the computer code, deriving from the plurality of retrieval commands and the responses a set of retrieval information, the set of

Art Unit: 2134

retrieval information comprising input vectors, characterizing the plurality of retrieval commands and converting the set of retrieval information into at least one rule for determining whether retrieval commands are acceptable) given the benefit of gathering, verifying and fine tuning a system.

For applicant's convenience the examiner provides a table illustrating steps that would be performed in a testing phase and matching anticipated (and later actual) steps of the intrusion system's operation.

TEST PHASE – Analysis	EXECUTION
Observing a plurality of retrieval commands that access the computer code Deriving responses to the plurality of retrieval commands generated by the computer code Observing a plurality of retrieval commands generated by the computer code Deriving from the plurality of retrieval commands and the responses a set of retrieval information, the set of retrieval information comprising input vectors	Generating retrieval information characteristic of data sent to a retriever by the computer code in response to a retrieval command issued by the retriever The retrieval information comprising an input vector characterizing the retrieval command
Characterizing the plurality of retrieval commands	Determining whether the retrieval command is acceptable using at least some of retrieval information as an input to at least one rule
Converting the set of retrieval information into at least one rule for determining whether retrieval commands are acceptable.	Responsive to the retrieval command being not acceptable performing at least one of the following: sending a message to a user or a computer.

9. As per claims 2-4, 16, the retrieval information comprises statistical information, and a retrieval vector comprises at least one of number of rows in the retrieval, number of columns in the retrieval, number of tables in the retrieval, identification of columns in the retrieval and identification of tables in the retrieval (e.g. col. 3 lines 58-60, col. 4 lines 55-67). The cited reference also clearly indicates the presence of a plurality of retrieval commands and the statistical information comprising at least one of the statistical characteristics specified by claim 6. The comparison disclosed by Mattsson in col. 3 line 38-col. 4 line 67 reads on an input vector containing parameterized information characteristic of the retrieval command accessing at least one rule recited by claim 7, and the limitations of claim 10 are met by col. 3 line 51-57 and col. 4 lines 16-25, and claim 12 by col. 5 lines 35-54, for example.
10. Claim 9 appears to address obvious variations of searching/data retrieval techniques well known in the art of database. Claim 9 refers to searching particular fields (e.g. columns, record etc.) using more than one value at the time and claim 11 addresses "pattern search", in which rather than a specific value, wildcard value is used. Additionally, the examiner points out that using more than one variable as an input disclosed by Mattsson and Oracle reads on the claim limitations, since each variable could be treated as a one dimensional vector. As a result having two variables in a query comprises at least two input vectors, wherein each input vector being associated with the same retrieval command.
11. Furthermore, as per claim 11, Mattsson does not disclose a canonicalized command that is a retrieval command stripped of literal field data (as defined in the

specification on pg. 7). However, using canonicalized commands that is command stripped of literal field data is old and well-known in the art of database searching (e.g. "Wild Characters", Oracle pg. 19-20). One of ordinary skill in the art at the time of applicant's invention would have been motivated to account for canonicalized commands stripped of literal field data in order to monitor/capture pattern searches.

12. As per claim 14, Mattsson does not explicitly disclose SQL commands. However, the SQL is one of the industry-standard languages for creating, updating and, querying relational databases. Thus, incorporate SQL commands into Mattsson's invention would have been obvious variations that are well known in the art. One would have been motivated to include these commands especially in light of the popularity and benefits of these commands as evidenced by their commercial success.

13. As per claim 12, Mattsson does not disclose sending an alert to a system administrator and updating an audit log. However, alerting administrator and login updating audit logs (updating logs that are used for audit) is well known in the computer security (see US 20040250127, for example), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include such features given the benefit of a prompt respond to a security threats as well as to analyze the causes and consequence of the threat.

14. As per claim 28, Mattsson does not disclose rules being provided by a system administrator. However, the limitation is implicit. System administrators administer systems: maintain, configure etc. Updating configuration, especially configuration

associated with system security is required since security threats as well as knowledge of them constantly evolves. Thus, any additional updates addressing additional known attacks (e.g. intrusion attacks) would have to involve an administrator (Note that in various system updates and configuration changes require administrative privileges).

15. As per claim 29, Mattsson does not disclose rules being provided by a vendor.

However, an ordinary artisan would recognize that various systems are provided with at least default configuration (e.g. configured by a vendor) and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to allow a vendor to provide at least one rule giving the benefit of speed and usability of setting up a new system.

16. As per claims 8, 17, 22 and 27, col. 2 lines 27-29 and col. 5 lines 35-54 clearly

suggests that the at least one rule is accessed from the group of techniques comprising real-time auditing and in-line interception, wherein at least one of: an alert is sent to a system administrator, audit log is updated, the command is not allowed to access the computer code; the command is allowed to access the computer code, but the access is limited, the command is augmented and a sender of the command is investigated is performed. As per claims 5 and 30, data (e.g. rules) in order to be accessed by computers must be kept in some form of a data structure, which reads on a table. Furthermore, in order for the data to be retrieved from a structure, the structure must exist (be pre-established). Even if a rule structure disclosed by Mattsson was not a "pure" table (e.g. a list which is a one-

dimensional table, or a database which is a collection of tables) the name of the structure would not affect the functionality of the invention, especially given the fact that using tables to store rules is an obvious variations well known in the art and that an ordinary artisan would have been motivated to use them especially in light of the benefits of use of tables as evidenced by their commercial success.

17. Furthermore, the examiner points out that, there are inherently two obvious choices of performing any actions, in real time and not in real time, wherein each option is an obvious variation of another. Given the fact that implementation of the steps discussed above in real time or not in real time would not affect the functionality of the invention as well as that real time operations are well known in the art of computing, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the real time training phase given the benefit of immediate feedback.

18. As per claims 20 and 23, Mattsson does not explicitly disclose using at least an API that accesses the computer code, code injection, patching, direct database integration or log file examination to extract the commands. However, using at least an API that accesses the computer code in communication involving computer processes (e.g. communicate with processes to extract particular values, e.g. commands) is well known in the art (e.g. application program interface, USPub 20030133554). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use at least an API that accesses the computer code,

code injection, patching, direct database integration or log file examination to extract the commands given the benefit of reduced complexity.

19. As per claim 21 and 24 Mattsson does not disclose interposing a proxy or a firewall between senders of the commands and the computer code. However, Official Notice is taken that it is old and well-known practice to interpose a proxy or a firewall between a client (e.g. a requester) and a server (e.g. database. See Pfleeger for example). One of ordinary skill in the art at the time of applicant's invention would have been motivated to interpose a proxy or a firewall between senders of the commands given the benefit of additional security.

20. The limitations of claims 18 and 26 are implicit. As discussed above, Mattsson's "detection phase" includes observing retrieval commands that access the computer code, responses to the retrieval commands generated by the computer and deriving from the responses a set of retrieval information in order to identify suspicious commands. Furthermore Sekar suggests comparing a detection phase with a training phase and in paragraph (Sekar, [0097]) discloses that the configuration data are gathered during the training session, which clearly indicates that any suspicious activity would have to be reported to an administrator.

21. As per claim 25, do not disclose determining duration of performing the training phase by statistical means. However, implementation of statistical evaluations is well known in the art of science (e.g. Weisstein, "Statistics", pg. 17-26) and it would have been obvious to one of ordinary skill in the art at the time of applicant's

Art Unit: 2134

invention to determine duration of performing the training phase by statistical means given the benefit of an optimal estimate using a limited number of information.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



9/16/07



KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER